

INFORMATION SECURITY and IT RISK MANAGEMENT

Manish Agrawal

Alex Campoe

Eric Pierce



WILEY

Information Security and IT Risk Management

Manish Agrawal, Ph.D.

Associate Professor

Information Systems and Decision Sciences

University of South Florida

Alex Campoe, CISSP

Director, Information Security

University of South Florida

Eric Pierce

Associate Director, Information Security

University of South Florida

WILEY

Vice President and Executive Publisher	Don Fowley
Executive Editor	Beth Lang Golub
Editorial Assistant	Jayne Ziemba
Photo Editor	Ericka Millbrand
Associate Production Manager	Joyce Poh
Cover Designer	Kenji Ngieng

This book was set by MPS Limited.

Founded in 1807, John Wiley & Sons, Inc. has been a valued source of knowledge and understanding for more than 200 years, helping people around the world meet their needs and fulfill their aspirations. Our company is built on a foundation of principles that include responsibility to the communities we serve and where we live and work. In 2008, we launched a Corporate Citizenship Initiative, a global effort to address the environmental, social, economic, and ethical challenges we face in our business. Among the issues we are addressing are carbon impact, paper specifications and procurement, ethical conduct within our business and among our vendors, and community and charitable support. For more information, please visit our website: www.wiley.com/go/citizenship.

Copyright © 2014 John Wiley & Sons, Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, website www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201)748-6011, fax (201)748-6008, website <http://www.wiley.com/go/permissions>.

Evaluation copies are provided to qualified academics and professionals for review purposes only, for use in their courses during the next academic year. These copies are licensed and may not be sold or transferred to a third party. Upon completion of the review period, please return the evaluation copy to Wiley. Return instructions and a free of charge return mailing label are available at www.wiley.com/go/returnlabel. If you have chosen to adopt this textbook for use in your course, please accept this book as your complimentary desk copy. Outside of the United States, please contact your local sales representative.

ISBN 978-1-118-33589-5 (paperback)

10 9 8 7 6 5 4 3 2

List of Figures

Figure 1.1: Classification of information security analysts	2
Figure 1.2: Time-consuming activities for information security professionals	4
Figure 1.3: Training needs identified by information security professionals	4
Figure 1.4: ILOVEYOU virus	7
Figure 1.5: T.J. Maxx	8
Figure 1.6: Defaced Georgian foreign ministry website	9
Figure 1.7: Google-China offices	10
Figure 1.8: Online Software Inspector	17
Figure 1.9: PC audit report	18
Figure 1.10: Contents of Downloads folder for Steganography exercise	19
Figure 1.11: Commands to hide text files at the end of image files	19
Figure 1.12: Manipulated images among original images	20
Figure 1.13: Opening image files in Notepad	20
Figure 1.14: Secret message hidden at the end of the image file	21
Figure 1.15: Sunshine State University funding sources	23
Figure 1.16: Extract from the organization structure of Sunshine State University	24
Figure 2.1: Paul Ceglia	32
Figure 2.2: Windows desktop usage—April 2013	33
Figure 2.3: System Center Operation Manager	34
Figure 2.4: Unix family tree	36
Figure 2.5: Albert Gonzalez, at the time of his indictment in August 2009	38
Figure 2.6: T J Maxx sales (2005–2010)	39
Figure 2.7: Virtual machine structure	41
Figure 2.8: VirtualBox download page	41
Figure 2.9: VirtualBox installer welcome screen	42
Figure 2.10: Default install Location	42
Figure 2.11: VirtualBox install confirmation	43
Figure 2.12: VirtualBox manager	43
Figure 2.13: Default setting for OS import	44
Figure 2.14: Virtual machine in Virtual machine manager	45
Figure 2.15: CPU error	45

Figure 2.16: Enabling PAE	46
Figure 2.17: Attach the VM to NAT	46
Figure 2.18: CentOS VM login screen	47
Figure 2.19: CentOS Linux desktop	47
Figure 2.20: Sunshine State University email infrastructure	50
Figure 3.1: Operating system structure	51
Figure 3.2: Reaching the command prompt window	53
Figure 3.3: Unix file hierarchy	54
Figure 3.4: vimtutor interface	67
Figure 3.5: Reaching users and groups manager	73
Figure 3.6: Adding users	74
Figure 3.7: Group manager	74
Figure 4.1: The basic information security model	83
Figure 4.2: Example CVE listing at the time of reporting	85
Figure 4.3: NVD entry for the CVE listing	86
Figure 4.4: ATLAS web interface	88
Figure 4.5: Phishing example	95
Figure 4.6: Adobe Flash zero-day exploit launched on February 28, 2011	96
Figure 4.7: Exploit usage	98
Figure 4.8: Using a browser on the VM	102
Figure 5.1: J-20 fighter	108
Figure 5.2: The elements of asset characterization	118
Figure 5.3: Generic IT asset life cycle	119
Figure 5.4: Student Information System	125
Figure 5.5: Uses of a hacked PC	133
Figure 6.1: Threat model	136
Figure 6.2: Threat agents over time by percent of breaches	137
Figure 6.3: External agents	137
Figure 6.4A: Chinese J-20 jet	138
Figure 6.4B: Lockheed F-22 jet	138
Figure 6.5: Internal agents	144
Figure 6.6: Partners	146
Figure 6.7: Edward Snowden	147
Figure 6.8: Datagram ISP goes down with Hurricane Sandy	149
Figure 6.9: Melissa error message	150
Figure 6.10: High level XSS attack	155

Figure 6.11: Bonzi buddy	158
Figure 6.12: Top vendor vulnerability breakdown	163
Figure 6.13: Firefox certificate exception	171
Figure 6.14: GSA main screen	171
Figure 6.15: New Task configuration	172
Figure 6.16: Starting a new scan	172
Figure 6.17: Viewing scan details	173
Figure 6.18: Report page	173
Figure 7.1: Encryption and decryption in context	177
Figure 7.2: Reference to Caesar cipher	178
Figure 7.3: Secret key cryptography overview	182
Figure 7.4: Public-key cryptography overview for data transmission	183
Figure 7.5: Using public-key encryption for digital signatures	184
Figure 7.6: Checksums example	186
Figure 7.7: Generic form of block encryption	188
Figure 7.8: Electronic code book	189
Figure 7.9: Cipher block chaining	190
Figure 7.10: Hash functions	194
Figure 7.11: Public-key certification process	195
Figure 7.12: CAs in browser	196
Figure 7.13: Untrusted certificate	197
Figure 7.14: GPG passphrase dialog	202
Figure 8.1: Identity and access management	208
Figure 8.2: Match/Merge flowchart	211
Figure 8.3: Smart card in a USB card reader	215
Figure 8.4: Hardware token	216
Figure 8.5: Fingerprint with minutia highlighted	219
Figure 8.6: Iris scanning in the Dubai Airport	220
Figure 8.7: Kerberos ticket exchange	224
Figure 8.8: Token-based authentication	226
Figure 8.9: Central authentication service	227
Figure 8.10: Discovery service for the InCommon federation	229
Figure 8.11: SSO with a SAML federation	230
Figure 8.12: OpenID	233
Figure 8.13: OpenID 2.0 provider selection screen	234
Figure 8.14: http://trendsmap.com	235
Figure 8.15: OAuth token passing	236

Figure 8.16:	Application UserId and ProviderUserId	237
Figure 8.17:	Intruder's attack path to military establishments	238
Figure 8.18:	Configuration QR code	243
Figure 8.19:	Google Authenticator (iOS)	244
Figure 9.1:	Access matrix example	252
Figure 9.2:	Typical firewall	253
Figure 9.3:	Perimeter firewalls and demilitarized zones	255
Figure 9.4:	Windows firewall blocking http	257
Figure 9.5:	Windows firewall allowing http	258
Figure 9.6:	Typical competitor console, circa 2003	267
Figure 9.7:	AirTight console, circa 2005	268
Figure 9.8:	/var/ossec/etc/ossec.conf (after change)	273
Figure 9.9:	OSSEC-WebUI	274
Figure 9.10:	Superb Fairy-Wrens, 40% success rate with security controls	275
Figure 11.1:	IRT interactions	311
Figure 11.2:	IRT communications	313
Figure 11.3:	DollSays	314
Figure 11.4:	Website defacement example	318
Figure 11.5:	PII search	319
Figure 11.6:	OSSEC, a popular file integrity tool	320
Figure 11.7:	Typical logs consolidated	321
Figure 11.8:	Log analysis	322
Figure 11.9:	End point protection example	323
Figure 11.10:	Containment, eradication, and recovery timeline	325
Figure 12.1:	Event Viewer Screen on Windows 8	334
Figure 12.2:	Summary of Administrative Events pane	335
Figure 12.3:	Recently viewed nodes	335
Figure 12.4:	Log Summary pane	335
Figure 12.5:	- Informational event screenshot	336
Figure 12.6:	Windows Administrative Events view	337
Figure 12.7:	syslog file evidence	339
Figure 12.8:	auth.log file	340
Figure 12.9:	Sample run of last	342
Figure 12.10:	Output of w command	343
Figure 12.11:	Security Log snapshot	346
Figure 12.12:	Log consolidation	347

Figure 12.13: Output of system info program	348
Figure 12.14: The sfc command	349
Figure 12.15: Windows MAC timestamps	351
Figure 12.16: File Explorer with timestamps	351
Figure 12.17: Sample timeline	352
Figure 12.18: Information Security and IT Risk Management is not affiliated with or otherwise sponsored by Dropbox, Inc.	353
Figure 13.1: Policy, standard, and guideline	364
Figure 13.2: Compliance	374
Figure 14.1: NIST 800-39 risk-management framework	386
Figure 14.2: Threat model	388
Figure 14.3: Risk assessment model	389
Figure 14.4: Sarbanes–Oxley auditing guidelines workflow for impact on IT	397

Preface

Unlike the problem facing the Superb Fairy-Wren (front cover), most information security problems we humans face are not matters of life and death (for more on the Wren's problem, please see the critical thinking question in chapter 9). However, they are vexing, expensive and frequent enough to make information security a contemporary profession and the topic of information security a worthwhile subject to study.

This book is designed to serve as the textbook for a one-semester course devoted to information security. It is focused on helping students acquire the skills sought in the professional workforce.

We start by introducing the professional environment of information security. After the student is convinced of the merits of the subject, the book introduces the basic model of information security consisting of assets, vulnerabilities, threats and controls. The rest of the course is devoted to characterizing assets, vulnerabilities and threats and responding to them using security controls. The book ends by integrating all these topics within the general umbrella of organizational risk management. At the end of the course, students should have an awareness of how information security concerns have evolved in our society and how they can use contemporary frameworks to respond to these concerns in a professional environment.

The book comes with a full set of end-of-chapter exercises. There are five kinds of exercises at the end of every chapter:

1. Traditional end-of-chapter questions are designed to improve student understanding and recall of common topics in information security.
2. An example case at the end of each chapter allows students to apply the knowledge in the chapter to business contexts.
3. There is a threaded design case running through all the chapters in the book. In this case, students play the role of the Chief Information Security officer of a typical state university and are confronted with situations related to the topics discussed in the chapter. They are required to analyze and evaluate the situation in light of the knowledge in the chapter to create a solution that addresses the present problem.
4. A critical thinking exercise introduces students to analogous situations and relate the ideas from the chapter to these situations. The problem confronting the Superb Fairy-Wren falls in this category.
5. Finally, each chapter has a detailed hands-on activity using a customized distribution of the CentOS Linux OS to be installed as a virtual machine using VirtualBox. We take great pride in this aspect of the book. We have carefully selected exercises that will help students become familiar not only with rudimentary information security tasks, but also with Linux systems administration. Eric in particular, has spent countless hours testing,

curating and maintaining the distribution. You may download the distribution from the textbook's companion website.

While the book is self-sufficient without the hands-on activity, this content is in direct response to employer demands and we do hope you will give your students the advantage of this aspect of the text. Chapters 2 and 3 introduce the basic setup and usage of the virtual machine. The instructions are detailed enough for students to be able to complete the exercises on their own.

When using the book, class time may be used in various ways. A traditional lecture format will work very well. Instructors interested in using class-time for more interactive activities will find that the end-of-chapter activities are a very useful way to use class time.

The author team integrates the different perspectives necessary to teach information security to an aspiring professional. Manish Agrawal is an MIS faculty member who designed this course and has taught it to MIS and Accounting students at the University of South Florida for over 5 years now. Alex Campoe is the Director of Information Security at the University of South Florida where he is at the frontline of the university's information security activities including incident response, policy development and compliance. Eric Pierce is responsible for identity management at the university. Many of the topics covered in the book are informed by their knowledge of the most important day-to-day activities that fall under the information security umbrella.

The Superb Fairy-Wren, though not strictly facing an information security problem, happens to use a solution that adopts many of the information security controls discussed in the text. The context also includes all the components of our basic information security model – assets in the form of the life of offspring, vulnerabilities in the form of delayed hatching, threats in the form of parasitic birds and controls including passwords. We think it succinctly describes the text.

We are eager to hear any comments you may have about the book – suggestions for improvement, errors and omissions, bugs in the virtual machine, and any other issues you may encounter. We will do our best to respond directly to you with corrections, and also address them as errata to be published on the textbook companion site. We obviously would also like to hear complementary things if the book helped improve your understanding of the subject, improved your teaching, helped you land a job, or helped you on the job. Those comments can give us indications on how to strengthen future editions of the book. Comments may be sent to the first author at magrawal@usf.edu.

Table of Contents

List of Figures	xi
Preface	xvii
Chapter 1 — Introduction	1
Overview	1
Professional utility of information security knowledge	1
Brief history	5
Definition of information security	11
Summary	14
Example case – Wikileaks, Cablegate, and free reign over classified networks	14
Chapter review questions.....	15
Example case questions.....	16
Hands-on activity – Software Inspector, Steganography.....	16
Critical thinking exercise: identifying CIA area(s) affected by sample real-life hacking incidents.....	21
Design case.....	21
Chapter 2 — System Administration (Part 1)	26
Overview	26
Introduction	26
What is system administration?.....	27
System administration and information security	28
Common system administration tasks	29
System administration utilities	33
Summary	37
Example case – T. J. Maxx	37
Chapter review questions.....	39

Example case questions.....	40
Hands-on Activity – Linux system installation	40
Critical thinking exercise – Google executives sentenced to prison over video	48
Design case.....	49
Chapter 3 — System Administration (Part 2)	51
Overview	51
Operating system structure	51
The command-line interface.....	53
Files and directories.....	53
Moving around the filesystem – pwd, cd	54
Listing files and directories	55
Shell expansions	56
File management	57
Viewing files.....	59
Searching for files.....	60
Access control and user management	61
Access control lists.....	64
File ownership	65
Editing files.....	66
Software installation and updates.....	67
Account management	72
Command-line user administration	75
Example case – Northwest Florida State College	77
Summary	78
Chapter review questions.....	78
Example case questions.....	79
Hands-on activity – basic Linux system administration.....	79
Critical thinking exercise – offensive cyber effects operations (OCEO).....	80
Design Case	80

Chapter 4 — The Basic Information Security Model	82
Overview	82
Introduction	82
Components of the basic information security model.....	82
Common vulnerabilities, threats, and controls.....	90
Example case – ILOVEYOU virus.....	99
Summary	100
Chapter review questions.....	100
Example case questions.....	101
Hands-on activity – web server security	101
Critical thinking exercise – the internet, “American values,” and security	102
Design case.....	103
Chapter 5 — Asset Identification and Characterization	104
Overview	104
Assets overview.....	104
Determining assets that are important to the organization	105
Asset types.....	109
Asset characterization.....	114
IT asset life cycle and asset identification	119
System profiling	124
Asset ownership and operational responsibilities.....	127
Example case – Stuxnet.....	130
Summary	130
Chapter review questions.....	131
Example case questions.....	131
Hands-on activity – course asset identification	132
Critical thinking exercise – uses of a hacked PC	132
Design case.....	133
Chapter 6 — Threats and Vulnerabilities	135
Overview	135
Introduction	135

Threat models	136
Threat agent	137
Threat action	149
Vulnerabilities	162
Example case – Gozi	167
Summary	168
Chapter review questions	168
Example case questions	168
Hands-on activity – Vulnerability scanning	169
Critical thinking exercise – Iraq cyberwar plans in 2003	174
Design case	174
Chapter 7 — Encryption Controls	176
Overview	176
Introduction	176
Encryption basics	177
Encryption types overview	181
Encryption types details	187
Encryption in use	194
Example case – Nation technologies	197
Summary	198
Chapter review questions	198
Example case questions	199
Hands-on activity – encryption	199
Critical thinking exercise – encryption keys embed business models	205
Design case	206
Chapter 8 — Identity and Access Management	207
Overview	207
Identity management	207
Access management	212
Authentication	213

Single sign-on.....	221
Federation.....	228
Example case – Markus Hess.....	237
Summary	239
Chapter review questions.....	239
Example case questions.....	240
Hands-on activity – identity match and merge.....	240
Critical thinking exercise – feudalism the security solution for the internet?	244
Design case.....	245
Chapter 9 — Hardware and Software Controls	247
Overview	247
Password management	247
Access control	251
Firewalls	252
Intrusion detection/prevention systems	256
Patch management for operating systems and applications	261
End-point protection.....	264
Example case – AirTight networks.....	266
Chapter review questions.....	270
Example case questions.....	270
Hands-on activity – host-based IDS (OSSEC).....	271
Critical thinking exercise – extra-human security controls.....	275
Design case.....	275
Chapter 10 — Shell Scripting	277
Overview	277
Introduction	277
Output redirection.....	279
Text manipulation.....	280
Variables	283
Conditionals.....	287

User input	290
Loops	292
Putting it all together	299
Example case – Max Butler.....	301
Summary	302
Chapter review questions.....	303
Example case questions.....	303
Hands-on activity – basic scripting	303
Critical thinking exercise – script security	304
Design case.....	305
Chapter 11 — Incident Handling	306
Introduction	306
Incidents overview.....	306
Incident handling.....	307
The disaster.....	327
Example case – on-campus piracy	328
Summary	330
Chapter review questions.....	330
Example case questions.....	331
Hands-on activity – incident timeline using OSSEC	331
Critical thinking exercise – destruction at the EDA	331
Design case.....	332
Chapter 12 — Incident Analysis	333
Introduction	333
Log analysis.....	333
Event criticality	337
General log configuration and maintenance.....	345
Live incident response.....	347
Timelines	350
Other forensics topics	352
Example case – backup server compromise.....	353

Chapter review questions.....	355
Example case questions.....	356
Hands-on activity – server log analysis.....	356
Critical thinking exercise – destruction at the EDA	358
Design case.....	358
Chapter 13 — Policies, Standards, and Guidelines	360
Introduction	360
Guiding principles	360
Writing a policy.....	367
Impact assessment and vetting	371
Policy review	373
Compliance.....	374
Key policy issues.....	377
Example case – HB Gary	378
Summary	379
Reference.....	379
Chapter review questions.....	379
Example case questions.....	380
Hands-on activity – create an AUP.....	380
Critical thinking exercise – Aaron Swartz.....	380
Design case.....	381
Chapter 14 — IT Risk Analysis and Risk Management	382
Overview	382
Introduction	382
Risk management as a component of organizational management	383
Risk-management framework	384
The NIST 800-39 framework	385
Risk assessment.....	387
Other risk-management frameworks	389
IT general controls for Sarbanes–Oxley compliance	391